Joseph G. Sansone
Jorge G. Tenreiro
Alison R. Levine
Russell J. Feldman
Karolina Klyuchnikova
U.S. Securities and Exchange Commission
New York Regional Office
100 Pearl Street
Suite 20-100
New York, NY 10004-2616
212-336-9144 (Feldman)
FeldmanR@sec.gov

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

SECURITIES AND EXCHANGE COMMISSION, **Plaintiff,** **-against-** **ROBERT B. WESTBROOK,** **Defendant.**	**Civil Action No.** **Complaint for Violations of the Federal Securities Laws** **Jury Trial Demanded**

Plaintiff Securities and Exchange Commission ("Commission"), located at 100 Pearl Street, Suite 20-100, New York, New York 10004-2616, alleges as follows against Robert B. Westbrook ("Westbrook" or the "Defendant"), whose last known address is 5B Radnor Walk, Chelsea, London SW3 4BP, United Kingdom:

SUMMARY

1. This is a "hack-to-trade" case. Specifically, this case involves a fraudulent scheme by Westbrook to hack into the computer systems of U.S. public companies to deceptively obtain material nonpublic information about their corporate earnings and to use that information to profit by trading in advance of the companies' public earnings announcements.

2. Between approximately January 2019 and August 2020 (the "Relevant Period"), Westbrook directly or indirectly made material misstatements and used deceptive means to access the computer systems of at least five companies with shares of stock publicly traded on U.S. securities exchanges (each a "Hacked Company" and collectively the "Hacked Companies").[1] This included that Westbrook: used the credentials of the Hacked Companies' employees without authorization (*e.g.*, usernames and passwords that did not belong to Westbrook); made affirmative misrepresentations that he was one of those employees or other legitimate user of the Hacked Companies' computer systems; and used tools and techniques to conceal his identity and location while conducting the hacking.

3. Westbrook gained unauthorized access into the Hacked Companies' computer systems to obtain pre-release corporate earnings information—including

[1] As explained further below, the "Hacked Companies" are identified herein as "Company-1," "Company-2," "Company-3," "Company-4," and "Company-5."

draft earnings releases, press releases, and scripts—and then used that information to trade in the securities of the Hacked Companies in advance of their public earnings announcements. Prior to these public earnings announcements, Westbrook established large and risky options positions in the Hacked Companies' securities, and often sold out of those positions shortly after the public earnings announcements.

4. In deceptively obtaining nonpublic earnings information from the Hacked Companies and trading in their securities in advance of at least 14 earnings announcements, Westbrook reaped approximately $3.75 million in illicit profits.[2]

5. By engaging in this conduct, Westbrook violated Section 10(b) of the Securities Exchange Act of 1934 ("Exchange Act") [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5].

NATURE OF THE PROCEEDINGS AND RELIEF SOUGHT

6. The Commission brings this action pursuant to the authority conferred upon it by Sections 21 and 21A of the Exchange Act [15 U.S.C. §§ 78u, 78u-1].

7. The Commission seeks a final judgment: (a) permanently enjoining Westbrook from violating the federal securities laws and rules this Complaint

[2] Westbrook's trades in advance of four of the 14 earnings announcements were unprofitable, even though he traded based on material nonpublic information. These unprofitable trades were excluded from the calculation of Westbrook's illicit profits.

alleges he has violated; (b) ordering Westbrook to disgorge all ill-gotten gains he received as a result of the violations alleged herein and to pay prejudgment interest thereon, pursuant to Sections 21(d)(3), 21(d)(5), and 21(d)(7) of the Exchange Act [15 U.S.C. §§ 78u(d)(3), 78u(d)(5), and 78u(d)(7)]; and (c) ordering Westbrook to pay a civil money penalty pursuant to Sections 21A(a) or 21(d) of the Exchange Act [15 U.S.C. §§ 78u-1, 78u(d)(3)]. The Commission seeks any other relief the Court may deem appropriate pursuant to Section 21(d)(5) of the Exchange Act [15 U.S.C. § 78u(d)(5)].

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to Sections 21(d), 21(e), 21A and 27 of the Exchange Act [15 U.S.C. §§ 78u(d), 77u(e), 78u-1, and 78aa]. Westbrook, directly or indirectly, made use of the means or instrumentalities of interstate commerce, or of the mails, or the facilities of a national securities exchange in connection with the transactions, acts, practices, and courses of business alleged in this Complaint. Westbrook deceptively obtained material nonpublic information from U.S. public companies and used the information to make securities trades that were cleared through U.S.-based brokerage firms and placed on multiple national securities exchanges, in a manner that used the instrumentalities of interstate commerce.

9. Venue lies in this District under Section 27 of the Exchange Act [15

U.S.C. § 78aa]. Certain of the purchases and sales of securities and acts, practices, transactions, and courses of business constituting violations alleged in this Complaint occurred within this District, and were effected, directly or indirectly, by making use of the means, instruments, or instrumentalities of transportation or communication in interstate commerce, or of the mails, or the facilities of national securities exchanges. Specifically, many of the illegal securities transactions were conducted using various national securities exchanges, such as the Nasdaq Global Market Select ("Nasdaq") and the New York Stock Exchange ("NYSE"), including one or more transactions that was processed using data servers located in New Jersey. Furthermore, under 28 U.S.C. § 1391(c)(3), venue lies in this District because Westbrook, as a foreign national residing outside the United States, may be sued in any judicial district.

DEFENDANT

10. **Robert B. Westbrook**, age 38, is a citizen and resident of the United Kingdom. Westbrook holds himself out as having studied economics at the University of Oxford, and he worked in several positions in the financial industry in London. During the Relevant Period, Westbrook held several brokerage accounts with firms based in the United States and held several brokerage accounts with firms in the United Kingdom.

TERMS USED IN THIS COMPLAINT

11. A stock option, commonly referred to as an "option," gives its purchaser-holder the right to buy or sell shares of an underlying stock at a specified price (the "strike" price) prior to the expiration date. Options are generally sold in "contracts," which give the option holder the opportunity to buy or sell 100 shares of the underlying stock.

12. A "call" option gives the purchaser-holder of the option the right, but not the obligation, to purchase a specified amount of an underlying security at a specified strike price within a specific time period. Generally, the buyer of a call option anticipates that the price of the underlying security will increase during a specified amount of time, allowing the buyer of the call option to make a profit from the difference between the higher market price of the underlying security and the strike price (less the cost of the option).

13. A "put" option gives the holder of the option the right, but not the obligation, to sell a specified amount of an underlying security at a specified strike price within a specific time period. Generally, the buyer of a put option anticipates that the price of the underlying security will decrease during a specified amount of time, allowing the buyer of the put option to make a profit from the difference between the strike price (less the cost of the option) and the lower market price of the underlying security.

14. An out-of-the-money call option refers to an option that would expire worthless unless the price of the underlying stock rose by a certain amount before expiration. Specifically, in the case of a call option, out-of-the-money refers to a scenario where the strike price is higher than the market price of the stock that underlies the call option.

15. An out-of-the-money put option refers to an option that would expire worthless unless the price of the underlying stock fell by a certain amount before expiration. Specifically, in the case of a put option, out-of-the-money refers to a scenario where the strike price is lower than the market price of the stock that underlies the put option.

16. Generally, the higher the strike price is above the stock price, the more inexpensive the call option will be to purchase. This is because it would take an upward move in the price of the underlying stock that is large enough to surpass the option's strike price for the call option to become in-the-money and become more valuable—and thus avoid expiring worthless. As a result, the higher the strike price of a call option is above the stock price, the greater the risk the call option will expire worthless.

17. Similarly, the nearer an out-of-the-money call option is to its expiration date, the greater the risk the call option will expire worthless. This results from the fact that there is simply less time for the price of the underlying

stock to rise enough to make the call option more valuable and avoid expiring worthless.

18. Likewise, the lower the strike price of a put option is below the stock price, the more inexpensive the put option will be to purchase. This is because it would take a downward move in the price of the underlying stock that is large enough to fall below the option's strike price for the put option to become in-the-money and become more valuable and thus avoid expiring worthless. As a result, the lower the strike price is below the stock price, the greater the risk the put option will expire worthless.

19. Similarly, the nearer an out-of-the-money put option is to its expiration date, the greater the risk the put option will expire worthless. This results from the fact that there is simply less time for the price of the underlying stock to fall enough to make the put option more valuable and avoid expiring worthless.

20. An "internet protocol address" or "IP address" is a unique number required for online activity conducted by a computer or other device connected to the internet. Computers use the unique identifier to send data to specific computers on a network. Often, IP addresses can be used to identify the geographic location of the server through which a computer accessed the internet. Thus, an IP address is like a return address on a letter. Additionally, an individual can conceal the IP

address from which he or she is accessing the internet through a number of different techniques and tools.

21. A "virtual private network" or "VPN" is one such tool that an individual can use to conceal his or her IP address. A VPN enables an individual to assume and use IP addresses different from his or her own, including IP addresses associated with different geographical regions.

FACTS

I. Overview of the Hack-to-Trade Scheme

22. During the Relevant Period, Westbrook engaged in an unlawful scheme in which he directly or indirectly used deceptive means to access the computer systems of at least five publicly-traded U.S. companies and then used that information to trade in advance of their earnings announcements.

23. Each of the Hacked Companies is a company that has shares of stock that are registered under Section 12(b) of the Exchange Act and that are publicly traded on a U.S. national securities exchange. In connection with their reporting obligations under the securities laws, the Hacked Companies prepared periodic and other reports to be filed with the Commission and disseminated to the investing public, including materials relating to the Hacked Companies' earnings. This included, among other things, drafts of earnings releases, press releases, and scripts for earnings announcements and related internal emails.

24. The information contained in these documents and emails was nonpublic because it had not yet been published or filed in a manner designed to achieve a broad dissemination to the investing public generally and without favoring any person or group.

25. The information contained in these documents and emails was also material. The Hacked Companies' information would have been important to the reasonable investor and viewed by the reasonable investor as having significantly altered the total mix of information made available. Information about a company's earnings is material because it relates to, among other things, a public company's financial condition, solvency, and profitability. For example, public disclosure of earnings information frequently leads to a change in the price of a company's stock. It is common for financial analysts to estimate and/or model a given company's quarterly or annual earnings. The market reaches a consensus expectation based in part on these different estimates. When a company releases its earnings announcements, the price at which shares of that company's stock trade often increases (if earnings exceed market expectations) or decreases (if earnings fall short of market expectations).

26. Westbrook knowingly, or with reckless disregard, made material misrepresentations, affirmatively misrepresented his identity, and employed a variety of deceptive and fraudulent devices, contrivances, artifices, practices,

means, and acts to access the computer systems of the five Hacked Companies. Specifically, Westbrook used, among other things: deceptively-obtained credentials of the Hacked Companies' employees; VPN services to conceal the IP address from which he accessed the internet; and anonymous email accounts to conceal his identity.

27. The hacking incidents each followed a similar pattern, with some limited exceptions, and occurred before the Hacked Companies were set to publicly announce earnings.

a. *First*, Westbrook reset a senior executive's computer system password at each of the Hacked Companies. Four of the five Hacked Companies used the same password reset portal software.

b. *Second*, Westbrook used the senior executive's username and reset password to access the Hacked Company's computer system, including the senior executive's Microsoft Office 365 ("Office 365") account and Microsoft Outlook email account ("Outlook"). In each hacking incident, the senior executive's Outlook contained emails with material nonpublic information about the Hacked Company's upcoming earnings announcement.

c. *Third*, Westbrook set up (or attempted to set up) email auto-forwarding rules in the senior executive's Outlook. Those rules were designed to forward emails containing nonpublic information about the Hacked Company's earnings from the senior executive's Outlook to one of several anonymous email accounts that Westbrook accessed.

d. *Fourth*, in advance of the Hacked Company's public earnings announcement, Westbrook purchased stock and/or options in the Hacked Company based on the nonpublic earnings information that he deceptively obtained.

e. *And finally*, Westbrook typically liquidated his securities positions in the Hacked Company shortly after its public earnings announcement and reaped significant profits.

28. Westbrook placed securities trades in the Hacked Companies on national securities exchanges through U.S.-based broker dealers, in a manner that utilized instrumentalities of interstate commerce.

29. By repeatedly engaging in this course of conduct—deceptively obtaining information from the Hacked Companies that he knew or recklessly disregarded was material and nonpublic and then trading in their securities in advance of their earnings announcements—Westbrook reaped approximately $3.75

million in illicit profits.

II. Examples of the Hack-to-Trade Scheme

30. Below are several examples where Westbrook deceptively obtained material nonpublic information from the Hacked Companies and traded profitably in the securities of the Hacked Companies based on that information.

A. Hack of Company-1

31. During the Relevant Period, Company-1 was a Delaware corporation headquartered in Orlando, Florida. It had a class of shares registered under Section 12(b) of the Exchange Act and its common stock traded on the NYSE.

32. On January 26, 2019, Westbrook hacked into Company-1's computer system by misrepresenting his identity and deceptively using the credentials of an employee of Company-1.

33. Specifically, Westbrook reset the password of a senior finance executive of Company-1 ("Executive-1") through Company-1's password reset portal. After he reset the password, Westbrook accessed Company-1's computer system, including Executive-1's Outlook.

34. While inside Company-1's computer system, Westbrook gained access to documents and emails containing material nonpublic information about Company-1's earnings for the fourth quarter of its fiscal year 2018. These emails included one that Executive-1 received on January 22, 2019, which contained a

draft press release about the company's fourth quarter financial results. The draft press release stated, among other things, that Company-1's net sales were down 14% and that its dividend would be $0.27 per share. The draft press release also forecast its fiscal year 2019 earnings per share in the range of $4.06 to $4.21. This was negative news because, by comparison, Company-1 paid a dividend of $0.68 per share in the prior quarter, and the consensus expectations of securities market analysts predicted earnings per share for the same period of $4.45.

35. While inside Executive-1's Outlook, Westbrook also created auto-forwarding rules designed to send all emails that Executive-1 received containing attachments to Aleksandrdubois1[@]gmail.com ("Aleksandrdubois")—an anonymous email account that Westbrook accessed. The auto-forwarding rules were likely unsuccessful, however, because Company-1's computer systems had been configured to prevent email auto-forwarding for all users.

36. Westbrook purchased Company-1's securities based on information he deceptively obtained and knew or recklessly disregarded was material and nonpublic regarding Company-1's financial results.

37. Starting on January 28, 2019 at approximately 3:20 pm EST—less than two days before Company-1 publicly announced its financial results for the fourth quarter of its fiscal year 2018—and continuing the next day, Westbrook purchased a total of 670 Company-1 put options across five different option series.

Specifically, Westbrook purchased the following Company-1 put options at a total cost of $129,429:

Put Options Purchased	Expiration Date	Strike Price
50	2/15/19	$30
110	2/15/19	$35
200	2/15/19	$40
230	3/15/19	$35
80	3/15/19	$40

38. The next day, on January 29, 2019, Westbrook sent an email to another individual stating, "Wanted to flag my idea on [Company-1], which I have reasonable conviction on (as reflected in the sizing relative to the portfolio) . . . this is my favorite idea – my view is there is significant guidance risk here."

39. On January 30, 2019, at approximately 7am EST, Company-1 reported its financial results for the fourth quarter of its fiscal year 2018 and announced the dividend it would be paying to shareholders. Those results reflected material information about Company-1's earnings that was included in the draft press release that Westbrook gained access to when he hacked into Company-1's computer system several days earlier, including that Company-1's net sales were down 14%, that its dividend would be 27 cents per share, and that the forecast for its fiscal year 2019 earnings per share was in the range of $4.06 to $4.21.

40. By the close of regular market trading that day, Company-1's stock price declined 27%—from a closing price of $38.13 on January 29, 2019 to a closing price of $27.67 on January 30, 2019.

41. On January 30, 2019, the same day that Company-1 reported its financial results, Westbrook sold his entire position of Company-1 put options for proceeds of $452,210. As a result of his trading in Company-1 securities in connection with this earnings announcement, Westbrook obtained a total profit of approximately $322,781.

42. The options positions Westbrook established in Company-1 prior to this earnings announcement were large and risky. Westbrook's purchases of Company-1 put options on January 28, 2019 accounted for approximately 16% of all Company-1 put options traded that day.[3] Similarly, Westbrook's purchases of Company-1 put options on January 29, 2019 accounted for approximately 32% of all Company-1 put options traded that day. In fact, going into Company-1's earnings announcement on January 30, 2019, Westbrook was the only retail holder of more than 200 Company-1 put options.

B. Hack of Company-2

43. During the Relevant Period, Company-2 was a Massachusetts corporation headquartered in Los Angeles, California. It had a class of shares registered under Section 12(b) of the Exchange Act and its common stock traded on the NYSE.

[3] Westbrook's purchases of Company-1 put options also accounted for approximately 78% of all Company-1 put options expiring in February 2019 that traded in the market on January 28, 2019.

44. On or about February 15, 2019, Westbrook hacked into Company-2's computer system. Company-2 used the same password reset portal software as Company-1, Company-4, and Company-5.

45. Specifically, Westbrook gained access to and set up an auto-forwarding rule in the Outlook email account of a senior accounting executive of Company-2 ("Executive-2"). That auto-forwarding rule was designed to send emails that Executive-2 received from any of four specified Company-2 employees to Harris.Slama402[@]aol.com ("Harris.Slama")—an anonymous email account that Westbrook accessed. That auto-forwarding rule began on or about February 15, 2019 and continued until at least January 2021.

46. As a result of the email auto-forwarding rule, Westbrook accessed emails containing material nonpublic information about Company-2's unreported financial results. For instance, emails auto-forwarded from Executive-2's Outlook to Harris.Slama between approximately April 30, 2020 and May 6, 2020 contained nonpublic information about Company-2's financial results for the first quarter of its fiscal year 2020. This forwarded information included an April 30, 2020 draft earnings call script, which stated, among other things, "Our first-quarter results were outstanding and well ahead of expectations"; the company "delivered double-digit revenue growth across all our segments"; "[r]evenue for the first quarter was $1.3 billion, up 30%"; and net income for "the first quarter of 2020 was $17.4

million, or $0.34 per diluted share." The forwarded information also included a May 1, 2020 draft Form 10-Q for the first quarter of its fiscal year 2020, which similarly reflected a revenue for the quarter of approximately $1.3 billion and diluted earnings per share of $0.34.

47. Westbrook purchased Company-2's securities based on information he deceptively obtained and knew or recklessly disregarded was material and nonpublic regarding Company-2's financial results.

48. Starting on May 4, 2020—two days before Company-2 was scheduled to announce its financial results—Westbrook purchased Company-2 stock and 3,706 Company-2 call options across eight different option series for a total cost of approximately $789,743. Specifically, Westbrook purchased 40,000 shares of Company-2 stock at a cost of $256,951, and the following Company-2 call options at a total cost of $532,792:

Call Options Purchased	Expiration Date	Strike Price
360	5/15/20	$5.00
818	5/15/20	$7.50
300	6/19/20	$5.00
1000	6/19/20	$7.50
200	10/16/20	$5.00
812	10/16/20	$7.50
200	12/18/20	$5.00
16	12/18/20	$7.50

49. On May 6, 2020, after the stock market closed, Company-2 announced its financial results for the first quarter of its fiscal year 2020. Those

results reflected material information about Company-2's earnings that was included in the draft earnings call script and draft Form 10-Q that Westbrook gained access to as a result of the email auto-forwarding rules he created in February 2019—such as revenue of $1.3 billion and diluted earnings per share of $0.34.

50. Company-2's earnings announcement reported higher revenue of $1.3 billion compared to consensus expectations of securities market analysts of $1.03 billion, and a higher diluted earnings per share number of $0.34 compared to consensus expectations of $0.06.

51. By the close of regular market trading the next day, Company-2's stock price had increased by approximately 30%—from a closing price of $6.19 on May 6, 2020 to a closing price of $8.03 on May 7, 2020.

52. On May 7, 2020, the day after Company-2 announced its financial results, Westbrook sold half of his Company-2 stock and approximately 40% of his Company-2 call options, obtaining a realized profit of approximately $101,343. As of the close of trading that day, Westbrook's remaining position in Company-2 securities had generated unrealized profits of approximately $209,141, for a total realized and unrealized gain of approximately $310,485.

53. The options positions Westbrook established in Company-2 prior to this earnings announcement were large and risky. Westbrook's purchases of

Company-2 call options between May 4, 2020 and May 6, 2020 accounted for approximately 70% of all Company-2 call options purchased between those dates. In fact, going into Company-2's earnings announcement on May 7, 2020, Westbrook owned more Company-2 call options than any other market participant. Westbrook's call options position was *more than six times* the size of the call options position of the next largest holder.

54. Notably, Westbrook traded in advance of Company-2's earnings announcements from on or about the time that Executive-2's emails were auto-forwarded to the Harris.Slama account in February 2019 until May 2020—a period when Westbrook was aware of material nonpublic information about Company-2's financial results.

55. All told, Westbrook obtained total profits of approximately $391,475 from his trading in Company-2 securities between May 2019 and May 2020.

C. <u>Hack of Company-3</u>

56. During the Relevant Period, Company-3 was a Delaware corporation headquartered in San Mateo, California. It had a class of shares registered under Section 12(b) of the Exchange Act and its common stock traded on the NYSE.

57. On February 21, 2019, Company-3 issued a press release stating that it would announce its financial results for the second quarter of its fiscal year 2019 on March 6, 2019 after market close.

58. The next day, on February 22, 2019, Westbrook hacked into Company-3's computer system by misrepresenting his identity and deceptively using the credentials of an employee of Company-3.

59. Specifically, Westbrook reset the computer system password of a senior finance executive of Company-3 ("Executive-3"). After he reset the password, Westbrook accessed Company-3's computer system, including Executive-3's Office 365 account and Outlook.

60. While inside Executive-3's Outlook, Westbrook created four auto-forwarding rules designed to send certain emails from Executive-3 to barnesbainesbjorn[@]gmail.com ("Barnesbainesbjorn")—an anonymous email account Westbrook accessed. In particular, the auto-forwarding rules were designed to forward, among others, emails containing attachments and Company-3's stock ticker in the email subject or body, as well as emails containing "script" in the email subject or body. Those auto-forwarding rules began to forward emails that same day and continued until approximately March 2021.

61. While inside Executive-3's Outlook, Westbrook gained access to documents and emails containing material nonpublic information about Company-3's financial results for the second quarter of its fiscal year 2019. This included a draft script of an earnings call that Executive-3 had received on February 19, 2019. That draft script stated, in part, that Company-3's "[t]otal revenue in the quarter of

$168.6 million was above the high-end of our guidance range" and that the quarter was "characterized by strong business momentum." Because of the email auto-forwarding rules that Westbrook created above, subsequent drafts of this earnings call script were also sent to the Barnesbainesbjorn account. This included a February 23, 2019 draft script, which stated that Company-3's "financial results exceeded our revenue and profitability guidance ranges, with total revenue of $169.3 million[.]"

62. Westbrook purchased Company-3's securities based on information he deceptively obtained and knew or recklessly disregarded was material and nonpublic regarding Company-3's financial results.

63. Starting on March 6, 2019 at 10:05am EST—the day that Company-3 was scheduled to announce its financial results—Westbrook bought 5,000 shares of Company-3 stock and 285 Company-3 call options across four different option series for a total cost of approximately $494,325. Specifically, Westbrook purchased 5,000 shares of Company-3 stock at a cost of $433,275, and the following Company-3 call options at a total cost of $61,050:

Call Options Purchased	Expiration Date	Strike Price
20	3/15/19	$85
190	3/15/19	$90
25	4/18/19	$85
50	4/18/19	$90

64. On March 6, 2019, after the stock market closed, Company-3

announced its financial results for the second quarter of its fiscal year 2019. Those results reflected material information about Company-3's earnings that was included in the draft earnings call script that Westbrook gained access to when he hacked into Company-3's computer system—such as total revenue for the second quarter of $169.3 million.

65. Company-3's earnings announcement exceeded the consensus expectations of securities market analysts, who had predicted that the company's total revenue for the quarter would be $159.71 million, as well as the company's previously issued guidance ranges.

66. By the close of regular market trading the next day, Company-3's stock price had increased 4.3%—from a closing price of $86.46 on March 6, 2019 to a closing price of $90.22 on March 7, 2019.

67. On March 7, 2019, shortly after the stock market opened, Westbrook sold all of his stock and call options in Company-3. As a result of his trading in Company-3's securities in connection with this earnings announcement, Westbrook obtained a total profit of approximately $236,492.

68. The options positions Westbrook established in Company-3 prior to this earnings announcement were large and risky. Westbrook's purchases of Company-3 call options on March 6, 2019 accounted for approximately 11% of all Company-3 call options traded that day. In fact, going into Company-3's earnings

announcement that day, Westbrook was, by far, the single largest retail holder of Company-3 call options.

69. Notably, Westbrook continued trading in advance of Company-3's earnings announcements during the period of time when Executive-3's emails continued to be auto-forwarded to the Barnesbainesbjorn account—from approximately March 2019 to approximately March 2020.

70. In one example, Westbrook bought $786,364 worth of Company-3 put options in advance of the company's second quarter earnings announcement that took place on March 4, 2020. He did so based on material nonpublic information about Company-3's financial results for the second quarter of its fiscal year 2020 that Westbrook gained access to because of the email auto-forwarding rule. This included a draft revenue forecast that reported second quarter revenue that was somewhat higher than analysts' consensus estimates ($174 million vs. $166.39 million), but also included forecasted revenue for its fiscal year 2020 that was significantly lower than analysts' consensus estimates ($724.7 million vs. $766.09 million). The earnings announcement reflected mixed news, where Company-3 beat certain quarterly expectations but significantly lowered its previous revenue guidance. By the close of business the next day, Company-3's stock price declined approximately 17%. Starting on March 5, 2020 and extending over several trading days, Westbrook liquidated his options position and obtained a total profit of

approximately $1.04 million.

71. All told, between March 2019 and March 2020, Westbrook obtained a total profit of approximately $1,422,015 from his trading of Company-3 securities while he was aware of material nonpublic information about Company-3's financial results.

D. Hack of Company-4

72. During the Relevant Period, Company-4 was a Delaware corporation headquartered in El Dorado, Arkansas. It had a class of shares registered under Section 12(b) of the Exchange Act and its common stock traded on the NYSE.

73. On October 23, 2019, Westbrook hacked into Company-4's computer system by misrepresenting his identity and deceptively using the credentials of an employee of Company-4.

74. Specifically, at approximately 7:19am EST, Westbrook reset the password of a senior accounting executive of Company-4 ("Executive-4") through Company-4's password reset portal—which used the same password reset portal software used by Company-1, Company-2, and Company-5. After he reset the password, Westbrook accessed Company-4's computer system, including Executive-4's Office 365 account and Outlook and Company-4's SharePoint

application.[4]

75. While inside Executive-4's Outlook, Westbrook created auto-forwarding rules designed to send certain emails from Executive-4 to Aleksandrdubois—the same anonymous email account that Westbrook used when setting up auto-forwarding rules in the hack of Company-1. In particular, the auto-forwarding rules were designed to forward any emails to Executive-4 that: (1) contained attachments and (2) were sent by Company-4's president or from an audit partner at an accounting firm. The auto-forwarding rules were unsuccessful, however, because Company-4's computer systems had been configured to prohibit email auto-forwarding.

76. Westbrook also deleted an email in Executive-4's Outlook account titled "Password Reset Acknowledgment" and an item called "Outlook Rules Organizer."

77. Furthermore, while inside Executive-4's Outlook, Westbrook gained access to documents and emails containing material nonpublic information about Company-4's financial results for the third quarter of its fiscal year 2019. This included an October 22, 2019 email containing a draft of Company-4's earnings release for that quarter. The draft earnings release stated, among other positive

[4] SharePoint is a collaboration platform offered by Microsoft, which allows employees to communicate, exchange information, and share files.

financial results, that Company-4's "Net income was $69.2 million, or $2.18 per diluted share, in Q3 2019 compared to net income of $45.0 million, or $1.38 per diluted share, in Q3 2018" and its "Adjusted EBITDA grew 51% over the prior year[.]"

78. Westbrook purchased Company-4's securities based on information he deceptively obtained and knew or recklessly disregarded was material and nonpublic regarding Company-4's financial results.

79. Starting on October 25, 2019 at approximately 12:15 pm EST—about two days after the hack described above—Westbrook began purchasing Company-4 call options. Between the time of the hack and Company-4's scheduled earnings announcement five days later, Westbrook purchased 1,342 Company-4 call options across eight different option series, the majority of which were out-of-the-money. Specifically, Westbrook purchased the following Company-4 call options for a total cost of $259,805:

Call Options Purchased	Expiration Date	Strike Price
100	11/15/19	$95
138	11/15/19	$100
326	11/15/19	$105
120	12/20/19	$90
184	12/20/19	$95
194	12/20/19	$100
230	12/20/19	$105
50	1/17/20	$90

80. On October 30, 2019, after the stock market closed, Company-4

reported its financial results for the third quarter of its fiscal year 2019. Those results reflected material information about Company-4's earnings that was included in the draft earnings release that Westbrook gained access to several days earlier when he hacked into Company-4's computer system, including that Company-4's net income was $69.2 million or $2.18 per diluted share, and its adjusted EBITDA grew 51% over the prior year.

81. Company-4's earnings announcement exceeded the consensus expectations of securities market analysts, who had predicted that Company-4 would report $1.46 earnings per diluted share for the quarter.

82. By the close of regular market trading the following day, Company-4's stock price increased more than 24%—from a closing price of $94.84 on October 30, 2019 to a closing price of $117.93 on October 31, 2019.

83. On October 31, 2019, shortly after the stock market opened, Westbrook sold all of his Company-4 call options. As a result of his trading in Company-4 securities in connection with this earnings announcement, Westbrook obtained a total profit of approximately $1,398,436.

84. The options positions Westbrook established in Company-4 prior to this earnings announcement were large and risky. Westbrook's purchases of Company-4 call options accounted for approximately 85% of all Company-4 call options traded between October 28, 2019 and October 30, 2019. In fact, going into

the earnings announcement on October 30, 2019, Westbrook owned more Company-4 call options than any other market participant and his call options position was more than twice the size of the next largest holder of call options.

E. Hack of Company-5

85. During the Relevant Period, Company-5 was a Delaware corporation headquartered in San Jose, California. It had a class of shares registered under Section 12(b) of the Exchange Act and its common stock was traded on Nasdaq.

86. On February 3, 2020, Westbrook hacked into Company-5's computer system by misrepresenting his identity and deceptively using the credentials of an employee of Company-5.

87. Specifically, at approximately 8:32am EST, Westbrook reset the password of a senior marketing executive of Company-5 ("Executive-5") through Company-5's password reset portal—which used the same password reset portal software used by Company-1, Company-2, and Company-4. After he reset the password, Westbrook accessed Company-5's computer system, including Executive-5's Office 365 account and Outlook, and Company-5's SharePoint and OneDrive applications.[5]

88. While inside Executive-5's SharePoint and OneDrive applications, Westbrook viewed documents containing material nonpublic information about

[5] OneDrive is an internet-based storage platform offered by Microsoft.

Company-5's financial results for the second quarter of its fiscal year 2020. For example, Westbrook accessed a draft letter from Company-5's CEO entitled "Q2 Earnings Email," which stated, in part, that it had been an "incredible quarter for [Company-5] with all time high record revenue, gross margin and operating margin." The documents Westbrook viewed also included a draft video script, titled "FY2020 Q2 Earnings Video Script," for Company-5's public earnings call that was scheduled to occur before the stock market opened the next day, February 4, 2020. The draft video script described Company-5's "record-breaking" second quarter results, stating, in part, the following: "Revenue: **$457.8M** (high end of guidance and new record); Gross Margin: **47.4%** (new record); Operating Margin: **28.8%** (well above guidance); [and] EPS [earnings per share]: **$1.53** (well above guidance)." (emphasis in original).

89. Westbrook also created an auto-forwarding rule in Executive-5's Outlook designed to send all of Executive-5's emails after the rule was set up to an anonymous email account, Harris.Slama—the same anonymous email account that Westbrook used to receive auto-forwarded emails in the hack of Company-2. The auto-forwarding rule was unsuccessful, however, because Company-5's computer systems had been configured to prohibit email auto-forwarding for all users.

90. Westbrook purchased Company-5's securities based on information he deceptively obtained and knew or recklessly disregarded was material and

nonpublic regarding Company-5's financial results.

91. Starting on February 3, 2020, at approximately 10:14am EST—less than two hours after the hack described above—Westbrook began purchasing Company-5 call options. Between the time of the hack and Company-5's scheduled earnings announcement the next morning, Westbrook purchased 1,917 Company-5 call options across nine different option series, the majority of which were out-of-the-money. Specifically, Westbrook purchased the following Company-5 call options for a total cost of approximately $492,802:

Call Options Purchased	Expiration Date	Strike Price
100	2/14/20	$80
500	2/14/20	$82
135	2/14/20	$85
361	2/28/20	$85
150	2/28/20	$90
170	3/20/20	$75
240	3/20/20	$77.50
200	3/20/20	$80
61	3/20/20	$85

92. On February 4, 2020, at 7:30am EST, Company-5 reported its financial results for the second quarter of its fiscal year 2020. Those results reflected material information about Company-5's earnings that was included in the drafts to which Westbrook gained access the day before when he hacked into Company-5's computer system, including revenue of $457.8 million, gross margin of 47.4%, operating margin of 28.8%, and earnings per diluted share of $1.53.

93. Company-5's earnings announcement exceeded the consensus expectations of securities market analysts, who had predicted that Company-5 would report adjusted earnings per share of $1.29.

94. By the close of regular market trading that day, Company-5's stock price increased 12%—from a closing price of $77.22 on February 3, 2020 to a closing price of $86.52 on February 4, 2020.

95. On February 4, 2020 at 9:31am EST—less than two hours after Company-5 reported its financial results—Westbrook began selling his Company-5 call options. By the close of regular market trading that day, Westbrook obtained a total realized and unrealized profit of $217,535 from his trading of Company-5 securities in connection with this earnings announcement.

96. The options positions Westbrook established in Company-5 prior to this earnings announcement were large and risky. Westbrook's purchases of Company-5 call options accounted for approximately 25% of all Company-5 call options traded on February 3, 2020. In fact, going into the earnings announcement on February 4, 2020, Westbrook owned more Company-5 call options than any other market participant.

III. Summary of Westbrook's Profits from Trading in the Hacked Companies

97. Westbrook's participation in this scheme was highly lucrative. Westbrook obtained approximately $3.75 million in illicit profits by trading in the

securities of the Hacked Companies prior to the release of at least 14 earnings announcements while he knew, or recklessly disregarded, that the information he deceptively obtained from the Hacked Companies was material and nonpublic.

98. The following table summarizes Westbrook's trading in connection with those 14 earnings announcements:

Issuer and Date of Earnings Announcement	Pre-Announcement Closing Equity Price	Post-Announcement Closing Equity Price	Equity Price % Change	Profit	Return
Company-1 1/30/2019	$38.13	$27.67	-27.43%	$322,781	249%
Company-3 3/6/2019	$86.46	$90.22	4.35%	$236,492	48%
Company-2 5/8/2019	$19.49	$17.05	-12.52%	$40,679	24%
Company-3 6/4/2019	$98.10	$95.15	-3.01%	$146,667	21%
Company-2 8/8/2019	$11.05	$9.98	-9.68%	$25,673	1%
Company-3 9/5/2019	$95.41	$109.41	14.67%	-$149,285	-49%
Company-4 10/30/2019	$94.84	$117.93	24.35%	$1,398,436	538%
Company-2 11/6/2019	$15.71	$18.47	17.57%	-$144,724	-58%
Company-3 12/5/2019	$119.33	$110.77	-7.17%	-$39,629	-1%

Issuer and Date of Earnings Announcement	Pre-Announcement Closing Equity Price	Post-Announcement Closing Equity Price	Equity Price % Change	Profit	Return
Company-5 2/4/2020	$77.22	$86.52	12.04%	$217,535	44%
Company-2 2/26/2020	$11.94	$12.07	1.09%	$14,639	74%
Company-3 3/4/2020	$112.48	$93.56	-16.82%	$1,038,855	132%
Company-2 5/6/2020	$6.19	$8.03	29.73%	$310,485	39%
Company-2 7/29/2020	$12.28	$12.32	0.33%	-$4,279	-18%
Total Profits (Excluding Losses)				**$3,752,242**	**91%**

IV. Westbrook Hacked into the Hacked Companies

99. Forensic data, blockchain data, and other data establish that Westbrook hacked into the Hacked Companies to obtain their nonpublic earnings information.

100. Westbrook's payment to and use of a VPN service provider ("VPN Service Provider-1") identifies Westbrook as the person who hacked into the Hacked Companies.

a. On October 22, 2019, Westbrook, through a Bitcoin wallet he

controlled, sent a Bitcoin payment equal to approximately $36.93 to VPN Service Provider-1 for a yearly subscription for its VPN services.

b. A subsequent email sent to one of the anonymous email accounts—Aleksandrdubois, which was used in the hacking of Company-1 and Company-4—confirmed that a yearly subscription to VPN Service Provider-1's VPN service commenced approximately twenty seconds after Westbrook sent that Bitcoin payment to VPN Service Provider-1.

c. That same day, VPN Service Provider-1's VPN service was used from the same IP address to sign into (i) one of the anonymous email accounts (Harris.Slama) that was used in the hacking of Company-2 and Company-5 and (ii) an email account (LoraineRanos796[@]aol.com) ("LoraineRanos") that was the recovery email account for two of the anonymous email accounts (Aleksandrdubois and Barnesbainesbjorn) used in the hacking of the Hacked Companies.

d. The next morning, VPN Service Provider-1's VPN service was used in the hack into Company-4's computer system described above.

e. About two days later, on October 25, Westbrook began purchasing call options in Company-4 in advance of its earnings announcement.

101. Moreover, Westbrook engaged in other conduct that further establishes him as the hacker in this hack-to-trade scheme.

a. During the Relevant Period, Westbrook used several VPN services. Each of the hacks discussed above took place using VPN services to which Westbrook subscribed. For example, on or about December 24, 2018, Westbrook purchased a yearly subscription to another VPN service provider ("VPN Service Provider-2"). The next month, an IP address attributed to VPN Service Provider-2 was used to access the Harris.Slama email account and the LoraineRanos email account. And during the Relevant Period, Westbrook had an active subscription to a third VPN service provider ("VPN Service Provider-3"). IP addresses attributed to VPN Service Provider-3 were used in the hacking of Company-5. IP addresses attributed to VPN Service Provider-3 were also used to access the Barnesbainesbjorn account, which was used in the hacking of Company-3.

b. During the Relevant Period, Westbrook made payments to an online directory service provider and an online genealogy company. Both of those companies provide personal and family information that could be used to guess the answers to the security questions that employees at the Hacked Companies may have used to reset their passwords.

c. Westbrook subscribed to at least five CAPTCHA[6] solving services. The self-service password reset portal software used by four of the five Hacked Companies allowed the companies to require CAPTCHA verification. CAPTCHA solving services would have helped Westbrook bypass verification requirements in his efforts to reset the passwords of the Hacked Companies' senior executives.

d. Westbrook purchased at least five highly technical hacker manuals, including "The Hacker Playbook 3: Practical Guide to Penetration Testing" and "Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World."

[6] CAPTCHA is a type of security measure known as a challenge-response authentication. It helps protect an account holder from password decryption by completing a basic test that proves the account holder is human and not a computer trying to break into a password protected account.

e. Westbrook opened over 50 email accounts, including anonymous email accounts hosted by overseas service providers known to be unreachable by law enforcement.

f. Westbrook purchased a vulnerability scanner, which is a software tool designed to permit a user to test and exploit the security of web applications.

g. Westbrook received email communications from online platforms known to sell hacking applications.

102. Finally, Westbrook previously admitted that he possessed the knowledge and technical computing skill to engage in acts akin to hacking. While employed at a financial firm, Westbrook accessed and downloaded an entire database from a third-party vendor—at a time when Westbrook and his colleagues were not expected to access the database. When an internal investigation at the financial firm revealed that Westbrook had downloaded the database, he admitted that he wrote a computer script that enabled him to download all the data on the database overnight.

V. Westbrook's State of Mind and Efforts to Conceal His Conduct

103. At all times relevant to this Complaint, Westbrook acted knowingly and/or recklessly in carrying out this scheme. He intended to hack into the

computer systems of the five Hacked Companies for the purpose of obtaining material nonpublic information.

104. Westbrook traded profitably in the securities of the Hacked Companies using the material nonpublic information he deceptively obtained, and he knew or recklessly disregarded that this information was material and nonpublic.

105. Westbrook repeatedly established large options positions in the Hacked Companies shortly before they were set to make their public earnings announcements. And those options positions were often out-of-the-money and/or were set to expire in the near term—increasing the risk that those options would expire worthless.

106. In addition, Westbrook sought to conceal his conduct from detection in a variety of ways. This included:

a. Using computer technology (such as VPN services) to hide his location;

b. Using affirmative misrepresentations to pose as others in order to access the computer systems of the Hacked Companies;

c. Deploying anonymous email accounts;

d. Deleting emails in a senior executive's account to cover up his hacking in Company-4.

107. Moreover, Westbrook received emails from a company that sells software to wipe evidence from devices. Those emails indicated that Westbrook had previously purchased this software.

108. This evidence shows that Westbrook acted with the requisite scienter when he executed this fraudulent scheme and took efforts to conceal his conduct.

VI. Conclusion

109. As detailed above, Westbrook executed a fraudulent hack-to-trade scheme. Westbrook deceptively obtained material nonpublic information from the Hacked Companies' computer systems and then used that information to trade profitably in the securities of the Hacked Companies in advance of their earnings announcements.

110. In perpetuating that fraudulent scheme, Westbrook made material misrepresentations, affirmatively misrepresented himself and his identity, and employed a variety of deceptive and fraudulent devices, contrivances, artifices, practices, means, and acts in order to access the computer systems of five Hacked Companies and to obtain nonpublic information about the Hacked Companies' earnings.

111. Westbrook did so for the purpose of using that information to trade in the securities of the Hacked Companies.

112. And Westbrook did just that. Based on deceptively-obtained

information that he knew or recklessly disregarded was material and nonpublic, Westbrook purchased the Hacked Companies' securities and then sold them following the Hacked Companies' earnings announcements, obtaining illicit profits of approximately $3.75 million.

CLAIM FOR RELIEF
Violations of Section 10(b) of the Exchange Act and Rule 10b-5 Thereunder

113. The Commission re-alleges and incorporates by reference here the allegations in paragraphs 1 through 112.

114. By engaging in the conduct described above, the Defendant knowingly or recklessly, in connection with the purchase or sale of securities, directly or indirectly, by the use of means or instrumentalities of interstate commerce, or the mails, or the facilities of a national securities exchange:

a. employed devices, schemes, or artifices to defraud;

b. made untrue statements of a material fact or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or

c. engaged in acts, practices, or courses of business which operated or would operate as a fraud or deceit upon any person.

115. By engaging in the foregoing conduct, the Defendant violated, and unless enjoined will continue to violate, Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5].

PRAYER FOR RELIEF

WHEREFORE, the Commission respectfully requests that the Court enter a Final Judgment:

I.

Permanently restraining and enjoining Westbrook and his agents, servants, employees and attorneys and all persons in active concert or participation with any of them from violating, directly or indirectly, Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule 10b-5(b) thereunder [17 C.F.R. §§ 240.10b-5(b)].

II.

Ordering Westbrook to disgorge all illicit profits, avoided losses, or other ill-gotten gains he received, directly or indirectly, with prejudgment interest thereon, as a result of the violations alleged in this Complaint, pursuant to Sections 21(d)(3), 21(d)(5), and 21(d)(7) of the Exchange Act [15 U.S.C. §§ 78u(d)(3), 78u(d)(5), and 78u(d)(7)].

III.

Ordering Westbrook to pay a civil penalty pursuant to Section 21A of the Exchange Act [15 U.S.C. § 78u-1] or, alternatively, to pay a civil penalty under

Section 21(d) of the Exchange Act [15 U.S.C. § 78u(d)].

IV.

Granting any other and further relief this Court may deem just, equitable, or necessary.

JURY DEMAND

The Commission demands a trial by jury.

Dated: New York, New York
September 27, 2024

/s/ Russell J. Feldman

Joseph G. Sansone
Jorge Tenreiro
Alison R. Levine
Russell J. Feldman
Karolina Klyuchnikova
U.S. Securities and Exchange Commission
New York Regional Office
100 Pearl Street
Suite 20-100
New York, NY 10004-2616
212-336-9144 (Feldman)
FeldmanR@sec.gov

Attorneys for Plaintiff
Securities and Exchange Commission

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

SECURITIES AND EXCHANGE COMMISSION, **Plaintiff,** **-against-** **ROBERT B. WESTBROOK,** **Defendant.**	**Civil Action No.** **DESIGNATION OF AGENT FOR SERVICE**

Pursuant to Local Rule 101.1(f), because the Securities and Exchange Commission (the "Commission") does not have an office in this district, the United States Attorney for the District of New Jersey is hereby designated as eligible as an alternative to the Commission to receive service of all notices or papers in the captioned action.

Therefore, service upon the United States or its authorized designee, David Dauenheimer, Deputy Chief, Health Care Fraud Unit, United States Attorney's Office for the District of New Jersey, 970 Broad Street, Suite 700, Newark, NJ 07102, shall constitute service upon the Commission for purposes of this action.

Respectfully submitted,

/s/ Russell J. Feldman

Joseph G. Sansone
Jorge G. Tenreiro
Alison R. Levine
Russell J. Feldman
Karolina Klyuchnikova
U.S. Securities and Exchange Commission
New York Regional Office
100 Pearl Street
Suite 20-100
New York, NY 10004-2616
212-336-9144 (Feldman)
FeldmanR@sec.gov

Attorneys for Plaintiff
Securities and Exchange Commission